

TALLINN
MANUAL
ON THE
INTERNATIONAL
LAW
APPLICABLE TO
CYBER
WARFARE

Prepared by the International Group of Experts
at the Invitation of The NATO
Cyber Defence Centre of Excellence

CAMBRIDGE



IDEAS. INFLUENCE. IMPACT.

The Tallinn Manual on the International Law Applicable to Cyber Warfare

On March 28th, the Atlantic Council, in partnership with the American Bar Association, will host the US launch of the *Tallinn Manual on the International Law Applicable to Cyber Warfare*. The project was sponsored by the NATO Cooperative Cyber Defense Center of Excellence. However, the conclusions drawn are those of the authors in their private capacities. Three organizations provided observers to the process: NATO, US Cyber Command, and the International Committee of the Red Cross.

Three Myths of the Tallinn Manual:

1. The Tallinn Manual is a NATO directive: **FALSE** — The project's conclusions are the opinions of the authors in their private capacities, and not a statement of official policy by NATO, any of its member governments, or any other participating organization.
2. According to the Tallinn Manual, Stuxnet was an act of war by the US: **FALSE** — Contrary to recent blog posts and articles, the International Group of Experts agreed that significant challenges stand in the way of definitively declaring Stuxnet an international armed conflict. The group was divided as to whether the operation had reached the threshold that allows a targeted State to exercise its inherent right of self-defense.
3. The Tallinn Manual gives governments permission to kill hackers: **FALSE** — While Rule 33 of the manual states: "[i]n case of doubt as to whether a person is a civilian, that person shall be considered to be a civilian," the International Group of Experts agreed that civilians directly participating in hostilities forfeit civilian protections. The group was, however, divided on how directly connected an act has to be to qualify as direct participation in hostilities. For example, whether the causal connection between the act of providing malware and a subsequent attack would be sufficiently direct to qualify as direct participation.

Key conclusions of the project:

- States may not knowingly allow cyber infrastructure located in their territory to be used for acts that adversely affect other States.
- States may be responsible for cyber operations directed against other States, even though those operations were not conducted by the security agencies. In particular, the **State itself will be responsible under international law for any actions of individuals or groups who act under its direction**. For instance, a State that calls on hacktivists to conduct cyber operations against other States will be responsible for those actions as if it had conducted them itself.
- The prohibition on the use of force in international law applies fully to cyber operations. Though international law has no well-defined threshold for determining when a cyber operation is a use of force, the International Group of Experts agreed that, at a minimum, any cyber operation that caused harm to individuals or damage to objects qualified as a use of force.
- The International Group of Experts agreed that cyber operations that merely cause inconvenience or irritation do not qualify as uses of force.

- States may respond to unlawful cyber operations that do not rise to the level of a use of force with countermeasures. Countermeasures are actions that would otherwise be unlawful were they not in response to the unlawful actions of another State. As an example, if one State disrupts communications in another, it **would be lawful for the target State to respond** by conducting disruptive cyber operations of its own.
- A State that is the victim of a cyber “armed attack” **may respond by using force**. The force may be either cyber or kinetic. In international law, an “armed attack” is a “grave” use of force. Any cyber operation that results in death or significant damage to property qualifies as an armed attack.
- The majority of the International Group of Experts agreed that non-State actors, such as cyber terrorists, are capable of conducting armed attacks, to which the victim State could respond in self-defense. In other words, **the matter is not solely one of law enforcement**. In certain circumstances, it would be permissible to use force against those cyber terrorist when they are located in other States.
- Under international law, it is possible that a conflict consisting entirely of cyber operations would qualify as an “armed conflict” to which international humanitarian law would apply. This is important because not only does international humanitarian law contain certain protections for individuals and objects during an armed conflict, but it also **gives immunity to combatants for certain actions**, such as intentionally killing the enemy, which would otherwise be unlawful.
- During an armed conflict, commanders and other superiors may be criminally responsible for ordering cyber operations that constitute war crimes or for failing to stop such operations when committed by their subordinates.
- Although there is no prohibition in international humanitarian law on civilians—such as hackers—conducting cyber operations during an armed conflict, if they do so, they sometimes become legitimate targets.
- Not all cyber operations directed against civilians and civilian objects are prohibited during an armed conflict. Instead, international humanitarian law primarily addresses operations that qualify as an “attack.”
- The majority agreed that **an attack is a cyber operation that causes injury or death to individuals** or damage or destruction to objects or which interferes with the functionality of cyber infrastructure in a manner that requires repair. Therefore, these experts would conclude that cyber operations directed against the civilian population or civilian objects are not prohibited by international humanitarian law when they merely cause disruption, irritation, and inconvenience.
- Directing a cyber operation against a civilian is a war crime if it injures the civilian or was likely to do so.
- It is unlawful to use cyber attacks to spread terror among the civilian population.
- Cyber weapons must be the subject of a legal review before they can be fielded on the battlefield.
- It is unlawful to launch a cyber attack that is not directed at a lawful target and which therefore would indiscriminately cause damage to civilians and civilian objects.
- During armed conflict, cyber operations must be employed against a target if they are militarily feasible in the circumstances and would result in less harm to civilians and civilian objects than the use of conventional weaponry.
- The special protections that medical and religious personnel, medical units, and medical transports have under international humanitarian law apply fully with respect to cyber operations directed against them. The same is true with regard to “objects indispensable to the survival of the civilian population” like medical supplies, food stores, and water treatment facilities.